ABSTRACT OF THE DISCLOSURE

In a buffer and a state included in a pseudorandom number generating apparatus, the state has the configuration of assuming that the unit length of data processing is n, the state has a size of 3 × n bits, and the buffer has a capacity of 32 × n bits, and according to clock control, a state transformation section (state transformation function) for conducting a state alteration from time t to time t+1 uses a nonlinear function F (having an n-bit input and an n-bit output) twice, or two different nonlinear functions F and G respectively once. The state transformation section has such a configuration that a nonlinear function such as a round function of a block cipher sufficiently evaluated as to the cryptographic security and implementation.